UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 17-CR-124

v.

MARCUS HUTCHINS,

Defendant.

DEFENDANT'S REPLY IN SUPPORT OF MOTION TO DISMISS THE FIRST SUPERSEDING INDICTMENT (FAILURE TO STATE OFFENSES AND MULTIPLICITY) (DOC. NO. 95)

In Counts One through Eight and Ten of the first superseding indictment, the government fails to allege any acts by defendant Marcus Hutchins which, if proven, would constitute violations of the law. The Court should dismiss these counts with prejudice.

1. **Counts One and Seven Fail to Allege Violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A)**

Defending the sufficiency of Counts One and Seven, the government first argues that it needs only to repeat verbatim the language of the invoked statutes to satisfy the pleading requirements of a federal criminal case. (Gov't Response at 3-4) (Doc. No. 100). The government confuses what is technically required with what is substantively necessary. The government's characterization of the

undisputed facts does not "constitute a violation of any statute," so there is "no case to prove." *United States v. Risk*, 843 F.2d 1059, 1060 (7th Cir. 1988). These counts are properly subject to dismissal for that reason.

Next, the government suggests that its characterization of Kronos and UPAS Kit as "malware" should satisfy the pleading standard, claiming that it is "common knowledge" that malware is "written with the intent of being disruptive or damaging." (Gov't Response at 5 (citing Oxford English Dictionary 2018).) But the Computer Fraud and Abuse Act (CFAA) does not make so-called malware illegal—it is not some form of contraband. In fact, the term "malware" does not appear anywhere in the charged statutes. The law is not concerned with what software is called, but what an actor uses it to do. Artificial labels aside, the question before the Court is whether Counts One and Seven adequately plead that Mr. Hutchins conspired or aided and abetted another to intentionally cause "damage" as defined by 18 U.S.C. § 1030(e)(8) —that is, "any impairment to the integrity or availability of data, a program, a system, or information."

Finally, the government's attempt to distinguish this case from the binding precedent of the Seventh Circuit is ineffective. The government offers *Fidlar Technologies v. LPS Real Estate Data Solutions* for the idea that "damage" as defined by the CFAA includes "clearly destructive behavior such as using a virus or worm or deleting data . . . [as well as] less obvious invasive conduct, such as

flooding an email account." (*Id.* at 5, citing 810 F.3d 1075, 1084 (7th Cir. 2016).) But the government does not argue that Kronos and UPAS Kit are viruses or worms, or that they delete data, or that they flood email accounts. The government alleges that Kronos and UPAS Kit recorded and exfiltrated data. (First Superseding Indictment ¶ 1(e) & (f).) This functionality is more like "simply download[ing] data without leaving a trace," which the court in *Fidlar Technologies* determined was *not* damage. *Id*. at 1084.

Finally, the rule of lenity counsels that the Court should reject the government's overbroad reading of "damage." Any ambiguity about the scope of a criminal statute should be resolved in favor of the defendant unless Congress clearly instructs otherwise. *Skilling v. United States*, 561 U.S. 358, 365 (2010).

2. Counts One Through Six Fail to Allege Violations of the Wiretap Act

In arguing that Kronos and UPAS Kit are "electronic, mechanical, or other devices" for purposes of the Wiretap Act, the government steers the Court's attention to legal issues that are not relevant to the issues Mr. Hutchins' motion raises.

The government notes that *Potter v. Havicek*—the case that most directly examines the issue of whether software alone can be a wiretapping device—deals with manufacturer liability for civil damages under § 2520, which creates a private right of action. (Gov't Response at 8-9, citing 2008 WL 2556723 (S.D. Ohio

June 23, 2008).) But since this is a criminal case, that aspect of *Potter* is irrelevant. What *is* relevant to this criminal case is *Potter's* conclusion that the software in that case was not an "electronic, mechanical, or other device" as defined by the Wiretap Act. 2008 WL 2556723, at **8-9. The government neglects to address this, a circumstance that does not turn on distinctions between civil and criminal liability.

The government contends that *United States v. Szymuszkiewicz* "did not address the issue in this case." (Gov't Response at 8-9, citing 622 F.3d 701, 707 (7th Cir. 2010) (as amended Nov. 29, 2010).) The government is correct that *Szymuszkiewicz* held that a device used to intercept a communication may be the same as the device used to receive that communication. 622 F.3d at 707. But the court there also held that the defendant acquired communications using computers. *Id*. The computers were the relevant devices for purposes of the offense. *Id*. Software was not.

The government also discusses several cases that considered whether software installed on computers "intercepted" communications within the meaning of the Wiretap Act, or accessed stored communications within the meaning of a different statute, the Stored Communications Act. (Gov't Response at 6-8, citing *Luis v. Zeng,* 2013 WL 811816, at **3-7 (S.D. Ohio March 5, 2013), *recommendation adopted, reversed on other grounds by* 833 F.3d 619 (6th Cir. 2016); *Shefts v. Petrakis,* No. 10-cv-1104, 2012 WL 4049484, at *9 (C.D. Ill. Sept. 13, 2012);

Klumb v. Goan, 884 F. Supp. 2d 644, 661 (E.D. Tenn. July 19, 2012).) But none of these cases addressed the critical question of whether the software or the computer was the relevant "device" for purposes of the Wiretap Act (since none of the defendants raised the issue, as Mr. Hutchins has).

That makes sense: those cases all involved claims that the defendants acquired communications using software running on a computer. Under those circumstances, a court has no reason to draw a distinction between the two because the software and computer work in tandem—the operation of one depends on the other. Indeed, the cases cited by the government discuss computers and the software installed on them as one unit. *See, e.g.*, *Zang*, 833 F.3d at 633 ("[O]nce installed on a computer, WebWatcher automatically acquires and transmits communications to servers"); *Klumb*, 884 F. Supp. 2d at 661 ("The point is that a program has been installed on the computer which will cause emails sent at some time in the future through the internet to be re-routed[.]"); *see also Shefts,* 2012 WL 4049484, **6-10 (variously referring to servers, email accounts, software, and BlackBerry smartphones as interception devices).

For purposes of the § 2512 charges in Counts Two through Five, however, the distinction between software and computer is important. In those counts, there is no computer, which would not be true in any scenario involving an actual interception. As noted in *Potter*, software alone is incapable of

intercepting anything: "It must be installed in a device, such as a computer, to be able to do so." 2008 WL 2556723, at *8.

The government also cites *United States v. Barrington* to support its position that keylogger software is a "electronic, mechanical, or other device" under the Wiretap Act. (Gov't Response at 8, citing 648 F.3d 1178, 1201 (11th 2011).) *Barrington*, however, says no such thing. That case considered whether a keylogger was "device-making equipment" or a "scanning receiver" under 18 U.S.C. § 1029, a statute that prohibits fraud and related activity in connection with access devices. *Id*. at 1201-02. That statute is not at issue in this case. In fact, the court in *Barrington* concluded there was *no* evidence that the keylogger was "a device or apparatus that can be used to intercept a wire or electronic communication in violation of [the Wiretap Act]." *Id*. at 1203. If anything, *Barrington* supports Mr. Hutchins' position.

The government also claims that Counts One, Two, Three and Six do not depend on the Kronos and UPAS Kit software in isolation qualifying as "electronic, mechanical, or other devices." (Gov't Response at 9-10.) The government first argues that Counts Two and Three should survive because Mr. Hutchins and Individual A allegedly linked to a YouTube video to demonstrate Kronos operating on a computer. (Gov't Response at 9.) But it is not alleged that Mr. Hutchins or Individual A actually made that video or performed any interception shown in it. Thus, according to the government, it is a crime to link

to a video someone else made that shows how malware functions on a computer. This, alone, is not disseminating an advertisement—it is simply displaying how a software program works. Section 2512(1)(c) does not make it illegal to show or describe how a device (much less software) functions; it makes it illegal to advertise the sale of certain devices.

And since § 2512(c)(1) is a restriction on speech, interpreting that section broadly to encompass any communication that demonstrates or describes how a device or software functions would present substantial First Amendment, vagueness, and overbreadth issues. The canon of constitutional avoidance counsels against an expansive construction of this statute. "[W]hen deciding which of two plausible statutory constructions to adopt, a court must consider the necessary consequences of its choice. If one of them would raise a multitude of constitutional problems, the other should prevail—whether or not those constitutional problems pertain to the particular litigant before the Court." *Clark v. Martinez*, 543 U.S. 371, 380-81 (2005).

Turning to Counts One and Six, the government argues that even if Kronos and UPAS do not qualify as "electronic, mechanical, or other devices," Mr. Hutchins transmitted and conspired to transmit the programs to others knowing and intending for the software to be used to intercept communications in violation of § 2511(1)(a). (Gov't Response at 10.) The government may be referring to the fact that § 2511(1)(a) prohibits "intentionally intercept[ing],

endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," and does not specifically mention the use of an "electronic, mechanical, or other device" to do so.

At first blush, § 2511(1)(a) might not appear to require such a device. But the Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication *through the use of any electronic, mechanical, or other device*." 18 U.S.C. § 2510(4) (emphasis added). In other words, it is impossible to "intercept" a communication within the meaning of § 2511(1)(a) without using an "electronic, mechanical, or other device" to do so. And if Kronos and UPAS Kit are not such devices, they cannot intercept communications in violation of § 2511.

The government may instead be arguing that Mr. Hutchins transmitted and conspired to transmit Kronos and UPAS Kit to others who could install the programs on computers, which could then intercept communications in violation of § 2511. Even assuming that others installed Kronos and UPAS Kit on computers that would qualify as devices, the allegations in Counts One and Six do not support the conclusion that Mr. Hutchins conspired to transmit or transmitted the programs to others knowing and intending for those people to intercept communications. The superseding indictment does not allege that Mr.

Hutchins intended a buyer to do anything in particular, as discussed in more detail below in Section 4.

Next, the government offers an array of dictionary definitions to argue that the common meanings of "device," "mechanism," and "apparatus" are more expansive than the dictionary definition of "device" offered by the defense. (Gov't Response at 11-12.) None of the government's suggested definitions say anything about software, nor do those definitions provide reason to conclude that software in isolation is an "electronic, mechanical, or other device."

The defense, on the other hand, has offered the Merriam-Webster dictionary definition that the court in *Potter* found to be the most germane for interpreting the Wiretap Act. 2008 WL 2556723, at *8. That court did not consider the more all-encompassing definitions (like those offered by the government) to be persuasive. *Id*.

Finally, the government contends that Congress drafted "electronic, mechanical, or other device" broadly "in order to accommodate changing technologies." (Gov't Response at 12-13.) In fact, Congress has been careful to limit the reach of §§ 2511 and 2512, increasing the level of mens rea in both statutes from "willful" to "intentional." Electronic Communications Privacy Act, Pub. L. 99-508, Title I, § 101(f), 100 Stat. 1853 (1986). And even though Congress has amended the Wiretap Act six times, it has never seen fit to expand the definition of "electronic, mechanical, or other device" to include software. When

Congress wishes to make something illegal, it knows how to do so—and it has not done so here. In the absence of any indication that Congress meant for the Wiretap Act to broadly encompass software, the rule of lenity directs that the Court should narrowly interpret the term "electronic, mechanical, or other device." *Skilling*, 561 U.S. at 365.

Moreover, computer source code is protected by the First Amendment. *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000) ("Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment."). Treating such code as a "device" for purposes of the Wiretap Act risks imposing criminal penalties on expressive activity, inviting the possibility of rendering the law unconstitutionally vague and overbroad. Here, again, the canon of constitutional avoidance weighs against expansive constructions of this statute, including treating software as a "device," which would "raise a multitude of constitutional problems." *Clark*, 543 U.S. at 380-81.

3. Counts Two and Three are Multiplicitous Because They Do Not Each Require Proof of a Fact Which the Other Count Does Not

The government argues that Counts Two and Three are not multiplicitous because "Count Three contains an additional element." (Gov't Response at 14.) But the proper inquiry is not whether *one count* contains an element that the other does not. It is "whether *each count* requires proof of a fact which the other does

not." *United States v. Conley*, 291 F.3d 464, (7th Cir. 2002) (citing *United States v. Briscoe*, 896 F.2d 1475 1522 (7th Cir. 1990)) (emphasis added).

Here, Counts Two and Three do not *each* require proof of an additional fact that the other does not: instead, they require proof of the same facts. Specifically, § 2512(1)(c)(i) prohibits the advertisement of an interception device when one *knows or has reason to know that the design of the device renders it primarily useful for the purpose of surreptitious interception*. And § 2512(1)(c)(ii) prohibits the advertisement of an interception device in a manner that *promotes its use for the purpose of surreptitious interception*. The same fact proves the offense charged in both counts: when one advertises a device designed for surreptitious interception, he promotes its use for surreptitious interception. That is the government's approach to Counts Two and Three. Thus, the facts necessary to prove these counts are the same.

When an indictment is multiplicitous, "it may prejudice the jury against the defendant by creating the impression of more criminal activity on his part than in fact may have been present." *United States v. Marquardt*, 786 F.2d 771, 778 (7th Cir. 1986) (quoting *United States v. Carter*, 576 F.2d 1061, 1064 (3rd Cir. 1978)). To avoid such prejudice, the Court should reject the government's suggestion to merge Counts Two and Three if they are found to be multiplicative. (Gov't Response at 14-15.) If the Court does not dismiss Count Three outright, it should at a minimum exercise its discretion to order the government to elect to proceed

with either Count Two or Count Three. *See United States v. Johnson*, 130 F.3d 1420, 1426 (10th Cir. 1997) (election avoids the possibility of falsely suggesting more criminal behavior to the jury than in fact occurred).

4. Counts One, Four Through Eight and Ten Fail to Allege the Requisite Intent

The government contends that Mr. Hutchins' final challenge to Counts One, Four Through Eight and Ten should be rejected because he actually challenges the sufficiency of the evidence anticipated at trial and attempts to apply civil pleading standards to a criminal indictment. (Gov't Response at 15-16.) But Mr. Hutchins' challenge is based not on the evidence anticipated at trial or civil pleading standards. It is based on the allegations in the superseding indictment and Seventh Circuit law. When "the government's characterization of the undisputed facts [does] not constitute a violation of any [federal] statute," dismissal of a case before trial is appropriate under Rule 12(b)(1). *United States v. Risk,* 843 F.2d 1059, 1060 (7th Cir. 1988).

The superseding indictment must state "the essential facts of the crimes charged." Fed. R. Crim. P. 7(c)(1). That standard is not watered down, as the government suggests, for inchoate offenses such as conspiracy, aiding and abetting, and attempt.

To engage in a conspiracy to violate a particular statute, a conspirator "must intend to further an endeavor which, if completed, would satisfy *all of the*

elements of a substantive criminal offense[.]" *Salinas v. United States*, 522 U.S. 52, 65 (1997) (emphasis added). Attempts are no different—they require an intent to carry out acts that satisfy each element of the relevant crime. *United States v. Morris*, 827 F.3d 696, 699 (7th Cir. 2016) (Hamilton, J., concurring). Likewise, a person can be liable for aiding and abetting only if he takes an affirmative act in furtherance of one element of an offense with the intent to facilitate the commission of the whole offense. *Rosemond v. United States*, 134 S. Ct. 1240, 1245 & 1248-49 (2014). That requisite intent "must go to the *specific and entire* crime charged." *Id*. at 1248 (emphasis added).

Counts One, Four Through Eight, and Ten share the same failure: they do not allege that Mr. Hutchins intended that each element of the relevant crime be committed. For example, Count Six alleges that Mr. Hutchins "knowingly and intentionally endeavored to intercept and procure any other person to intercept and endeavor to intercept" certain electronic communications. But the superseding indictment does not allege that Mr. Hutchins intended the sale of Kronos to have any specific result, much less that he knew or intended for the buyer to use Kronos to intercept certain electronic communications.

Count Seven suffers from the same flaw. Mr. Hutchins is accused of knowingly causing and aiding and abetting the transmission of a program, information, code, and command and as a result attempting to cause damage to protected computers. But to violate § 1030(a)(5)(A), one must *intentionally* cause

damage to a protected computer. Attempting a violation of that statute requires the intent to intentionally cause damage to a protected computer. Aiding and abetting a violation likewise requires the intent to intentionally cause damage to a protected computer. But again, it is not alleged that Mr. Hutchins intended the sale of Kronos to produce any particular outcome, much less that they intended to damage a protected computer.

Count Eight is similarly deficient. It charges that Mr. Hutchins knowingly aided and abetted another to intentionally access a computer without authorization, thereby obtaining and attempting to obtain information from a protected computer for private financial gain. Once again, to violate the statute, Mr. Hutchins would have had to intend for another to intentionally access a computer without authorization and obtain information. There is no allegation in the superseding indictment that he intended any such thing.

Count Ten suffers from the same problems. It alleges that Mr. Hutchins knowingly conspired and agreed with Individual A and others to violate § 1343. Conspiracy to violate this statute requires Mr. Hutchins to have had the specific intent to devise and participate in a scheme to defraud and obtain money by means of false and fraudulent pretenses and to make transmissions in interstate or foreign commerce for the purpose of executing the scheme. The superseding indictment does not support such a theory.

And Count One fails for the same reasons articulated above with respect to Counts Six, Seven, and Eight. There, Mr. Hutchins is charged with conspiring to violate 18 U.S.C. §§ 1030(a)(5)(A), (a)(2)(C) and 2511(1)(a). Conspiring to violate these statutes requires the intent to further an endeavor which, if completed, would intentionally 1) cause damage to a computer, 2) access a computer without authorization, and 3) intercept, endeavor to intercept and procure any other person to intercept and endeavor to intercept an electronic communication. As described above, the allegations do not establish such a case.

***

The superseding indictment's infirmities are fatal to the government's ability to move forward with Counts One Through Eight and Ten. Mr. Hutchins therefore respectfully asks that those counts be dismissed with prejudice.

DATED: August 3, 2018

Respectfully submitted,

/s/ Marcia Hofmann

MARCIA HOFMANN
Zeitgeist Law PC
25 Taylor Street
San Francisco, CA 94102
Email: marcia@zeitgeist.law
Telephone: (415) 830-6664

/s/ Brian E. Klein
BRIAN E. KLEIN
Baker Marquart LLP
2029 Century Park E – Suite 1600
Los Angeles, CA 90067
Email: bklein@bakermarquart.com
Telephone: (424) 652-7800

/s/ Daniel W. Stiller
DANIEL W. STILLER
DStillerLLC
Box 511130
Milwaukee, WI 53203
Email: dan@dstillerllc.com
Telephone: (414) 207-3190

Attorneys for Marcus Hutchins